兵庫県教育情報セキュリティ対策基準

第１節　趣旨

第１条　この対策基準は、兵庫県教育委員会行政組織規則（昭和58年教育委員会規則第９号）第３条第３項に規定する県立学校（以下「学校」という。）における情報セキュリティを確保するため、兵庫県情報セキュリティ対策指針（平成15年政策会議決定）第２章について、特別の情報セキュリティ対策基準を定めるものである。

２　兵庫県情報セキュリティ対策指針第１章及びこの対策基準をもって兵庫県（以下「県」という。）の教育情報セキュリティポリシーとする。

第２節　対象範囲及び用語説明

（適用範囲）

第２条　教育情報セキュリティポリシーは、学校の情報資産に係る業務に携わるすべての職員を対象とする。

（情報資産の範囲）

第３条　この対策基準が対象とする情報資産は、次のとおりとする。

(1) 教育情報ネットワーク、教育情報システム、これらに関する設備、電磁的記録媒体

(2) 教育情報ネットワーク及び教育情報システムで取り扱う情報（これらを印刷した文書を含む。）

(3) 教育情報システムの仕様書及び教育情報ネットワーク図等のシステム関連文書

（用語説明）

第４条　この対策基準における用語は、次の表に掲げるとおりとする。

用語	定義
校務系情報	児童生徒の成績、出欠席及びその理由、健康診断結果、指導要録、教職員の個人情報など、学校が保有する情報資産のうち、それら情報を学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用することを想定しており、かつ、当該情報に児童生徒がアクセスすることが想定されていない情報
校務外部接続系情報	校務系情報のうち、保護者メールや学校ホームページ等インターネット接続を前提とした校務で利用される情報
学習系情報	児童生徒のワークシート、作品など、学校が保有する情報資産のうち、それら情報を学校における教育活動において活用することを想定しており、かつ当該情報に教職員及び児童生徒がアクセスすることが想定されている情報
教員用端末	校務系情報にアクセス可能な端末で、仮想デスクトップから校務系情報にアクセス可能な校務用端末
	学習系情報にアクセス可能な端末で、教職員のみが利用可能な指導者用端末
学習者用端末	学習系情報にアクセス可能な端末で、児童生徒が利用する端末（児童生徒が所有する端末を含む。）
校務系システム	校務系ネットワーク、校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステム

校務外部接続系システム	校務外部接続系ネットワーク、メールサーバ、ホームページ運用サーバ及び校務用端末等から構成される校務外部接続系情報を取り扱うシステム
学習系システム	学習系ネットワーク、学習系サーバ、学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム
教育情報システム	校務系システム、校務外部接続系システム及び学習系システムを合わせた総称
教育情報ネットワーク	兵庫県教育情報ネットワーク（学校からの回線で直接インターネットへ接続するものを含む。）
校務系サーバ	校務系情報を取り扱うサーバ
校務外部接続系サーバ	校務外部接続系情報を取り扱うサーバ
学習系サーバ	学習系情報を取り扱うサーバ

第３節　組織体制

（最高情報セキュリティ責任者）

第５条　教育次長を最高情報セキュリティ責任者（Chief Information Security Officer、以下「CISO」という。）とする。

２　CISOは、県における全ての教育情報ネットワーク、教育情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

（統括教育情報セキュリティ責任者）

第６条　教育企画課長をCISO直属の統括教育情報セキュリティ責任者とする。統括教育情報セキュリティ責任者はCISOを補佐しなければならない。

２　統括教育情報セキュリティ責任者は、教育情報ネットワーク及び教育情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

３　統括教育情報セキュリティ責任者は、教育情報ネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

４　統括教育情報セキュリティ責任者は、県において所有している教育情報システムについて、教育情報セキュリティポリシーの遵守に関する意見の集約を行う。

５　統括教育情報セキュリティ責任者は、教育情報セキュリティ管理者、教育情報システム管理者及び教育情報システム管理者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

６　統括教育情報セキュリティ責任者は、県の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISOの指示に従い、CISOが不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。

７　統括教育情報セキュリティ責任者は、県の共通的な教育情報ネットワーク、教育情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

８　統括教育情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、教育情報セキュリティ責任者、教育情報セキュリティ管理者、教育情報システム管理者、教育情報システム管理者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

９　統括教育情報セキュリティ責任者は、緊急時にはCISOに早急に報告を行うとともに、回復のための対策を講じなければならない。

（教育情報セキュリティ責任者）

第７条　教職員人事課長を教育情報セキュリティ責任者とする。

２　教育情報セキュリティ責任者は、教職員に対する教育、訓練、助言及び指示を行う。
３　教育情報セキュリティ責任者は、教育情報セキュリティ管理者から報告を受けた情報セキュリティインシデントについて適切な措置を講じる。

（教育情報セキュリティ管理者）
第８条　校長を教育情報セキュリティ管理者とする。
２　教育情報セキュリティ管理者は、当該学校の情報セキュリティ対策に関する権限及び責任を有する。
３　教育情報セキュリティ管理者は、当該学校の情報セキュリティ実施手順の策定及び維持・管理を行う。
４　教育情報セキュリティ管理者は、当該学校において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、CISO及び統括教育情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

（教育情報システム管理者）
第９条　県立総合教育センター長を教育情報システム管理者とする。
２　教育情報システム管理者は、所管する教育情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。
３　教育情報システム管理者は、所管する教育情報システムにおける情報セキュリティに関する権限及び責任を有する。
４　教育情報システム管理者は、所管する教育情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

（教育情報システム担当者）
第10条　県立総合教育センター情報教育研修課長を教育情報システム担当者とする。
２　教育情報システム担当者は、教育情報システム管理者の指示等に従い、教育情報システムの開発、設定の変更、運用、更新等の作業を行う。

（学校教育情報セキュリティ・システム担当者）
第11条　教育情報セキュリティ管理者は、当該学校の教職員の中から学校教育情報セキュリティ・システム担当者を指名する。
２　学校教育情報セキュリティ・システム担当者は、教育情報セキュリティ管理者の指示に従い、学校における教育情報システムの導入・管理・運用等を補助する。

（教育情報セキュリティ対策委員会）
第12条　学校の情報セキュリティ対策を統一的に行うため、県で設置する教育情報セキュリティ対策委員会（以下「対策委員会」という。）において、この対策基準等、情報セキュリティに関する重要な事項を決定する。

（学校教育情報セキュリティ・システム委員会）
第13条　学校の教育情報ネットワーク、教育情報システム等の運用及びそこで取り扱う情報資産の管理を適切に行うため、各学校に学校教育情報セキュリティ・システム委員会を設置する。

（情報セキュリティに関する統一的な窓口の設置）
第14条　CISOは、情報セキュリティの統一的な窓口の機能を有する組織（以下「情報セキュリティに関する統一的な窓口」という。）を整備し、情報セキュリティインシデントについて学校等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備する。

２　教育企画課は、CISOによる情報セキュリティ戦略の意思決定が行われた際には、その内容を関係者及び学校等に提供する。
３　教育企画課は、情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。
４　教育企画課は、情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行う。

第４節　情報資産の分類と管理方法

（情報資産の分類）
第15条　学校における情報資産は、機密性、完全性及び可用性を踏まえ、セキュリティ侵害が及ぼす影響の大きさにより、次の表に揚げるとおり重要性に基づいて分類し、必要に応じて取扱制限を行うものとする。

分類	分類基準
重要性Ⅰ	セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼすもの（秘匿情報）
重要性Ⅱ	セキュリティ侵害が学校事務及び教育活動の実施に影響を及ぼすもの（保護情報）
重要性Ⅲ	セキュリティ侵害が学校事務及び教育活動の実施に影響を及ぼさないもの（公開情報）

（情報資産の管理）
第16条　教育情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。
２　情報資産が複製又は伝送された場合には、複製等された情報資産も前条の分類に基づき管理しなければならない。
３　教職員は、情報資産について、その分類を表示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。
４　教職員は、業務上必要のない情報を作成してはならない。
５　情報を作成する者は、情報の作成時に前条の分類に基づき、当該情報の分類と取扱制限を定めなければならない。
６　情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。
７　学校内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。
８　学校外の者が作成した情報資産を入手した者は、前条の分類に基づき、当該情報の分類と取扱制限を定めなければならない。
９　情報資産を入手した者は、その情報資産の分類が不明な場合、教育情報セキュリティ管理者に判断を仰がなければならない。
10　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。
11　情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。
12　情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。
13　教育情報セキュリティ管理者及び教育情報システム管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。

14　教育情報セキュリティ管理者及び教育情報システム管理者は、情報資産を記録した電磁的記録媒体を保管する場合は、書込禁止の措置を講じなければならない。
15　教育情報セキュリティ管理者及び教育情報システム管理者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管するよう考慮しなければならない。
16　電子メール等により重要性Ⅱ以上の情報資産を外部送信する者は、限定されたアクセスの措置設定を行わなければならない。
17　車両等により重要性Ⅱ以上の情報資産を運搬する者は、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。
18　重要性Ⅱ以上の情報資産を運搬する者は、教育情報セキュリティ管理者に許可を得なければならない。
19　重要性Ⅱ以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。
20　重要性Ⅱ以上の情報資産を外部に提供する者は、教育情報セキュリティ管理者に許可を得なければならない。
21　教育情報セキュリティ管理者は、住民に公開する情報資産について、完全性を確保しなければならない。
22　重要性Ⅱ以上の情報資産を廃棄する者は、情報を記録している電磁的記録媒体が不要になった場合、電磁的記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなければならない。紙媒体が不要となった場合は、焼却、裁断、溶解等により廃棄しなければならない。
23　情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。
24　情報資産の廃棄を行う者は、教育情報セキュリティ管理者又は教育情報システム管理者の許可を得なければならない。

第５節　物理的セキュリティ

（物理的セキュリティ）
第17条　教育情報システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、ほこり、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

（サーバの冗長化）
第18条　教育情報システム管理者は、校務系サーバその他の校務系情報を格納しているサーバを冗長化し、同一データを保持しなければならない。また、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。
２　教育情報システム管理者は、学習系サーバその他の学習系情報を格納しているサーバのハードディスクを冗長化しなければならない。

（機器の電源）
第19条　教育情報システム管理者は、統括教育情報セキュリティ責任者及び外部委託業者と連携し、校務系サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。
２　教育情報システム管理者は、統括教育情報セキュリティ責任者及び外部委託業者と連

携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

（通信ケーブル等の配線）

第20条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、外部委託事業者と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。

２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、外部委託事業者から損傷等の報告があった場合、連携して対応しなければならない。

３　統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

４　統括教育情報セキュリティ責任者及び教育情報システム管理者は、自ら又は教育情報システム管理者及び契約により操作を認められた外部委託事業者以外の者が配線を変更又は、追加できないように必要な措置を施さなければならない。

（機器の定期保守及び修理）

第21条　教育情報システム管理者は、重要性Ⅱ以上の情報資産を取り扱うサーバ等の機器の定期保守を実施しなければならない。

２　教育情報システム管理者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、教育情報システム管理者は、外部の事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するとともに、秘密保持体制の確認等を行わなければならない。

（施設外又は学校外への機器の設置）

第22条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、施設外又は学校外にサーバ等の機器を設置する場合、CISOの承認を得なければならない。

２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（機器の廃棄等）

第23条　教育情報セキュリティ管理者及び教育情報システム管理者は、機器を廃棄又はリース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

（管理区域の構造等）

第24条　管理区域とは、ネットワークの基幹となる機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋（以下「情報システム室」という。）及び電磁的記録媒体の保管庫をいう。

２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、外部委託業者と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

３　統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

４　統括教育情報セキュリティ責任者及び教育情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしな

ければならない。

（管理区域の入退室管理等）

第25条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、管理区域への入退室を許可された者のみに制限し、入退室管理簿の記載による入退室管理を行わなければならない。

２　情報システム担当職員及び外部委託事業者が、管理区域に入室することを許可する場合、これらの者に身分証明書等を携帯させ、必要に応じ、その提示を求めなければならない。

３　統括教育情報セキュリティ責任者及び教育情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された情報システム担当職員等が付き添うものとし、外見上情報システム担当職員等と区別できる措置を講じなければならない。

４　統括教育情報セキュリティ責任者及び教育情報システム管理者は、重要性Ⅱ以上の情報資産を取り扱うシステムを設置している管理区域について、当該情報システムに関連しないコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

（機器等の搬入出）

第26条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報システム室へ搬入する機器等が、既存の情報システムに与える影響について、あらかじめ教育情報システム管理者又は外部委託業者に確認を行わせなければならない。

２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報システム室の機器等の搬入出について、情報システム担当職員等を立ち会わせなければならない。

（通信回線及び通信回線装置の管理）

第27条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、施設内の通信回線及び通信回線装置を適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

３　統括教育情報セキュリティ責任者及び教育情報システム管理者は、重要性Ⅱ以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

４　統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

５　統括教育情報セキュリティ責任者及び教育情報システム管理者は、重要性Ⅱ以上の情報資産を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。

（教員用端末の管理）

第28条　教育情報セキュリティ管理者は、盗難防止のため、教員用端末の管理について、物理的措置を講じるとともに、情報資産管理ファイルをもとに、適切な管理を行わなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

２　教育情報システム管理者は、教育情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

（学習者用端末の管理）

第29条　統括教育情報セキュリティ責任者、教育情報システム管理者及び教育情報セキュリティ管理者は、児童生徒が所有するパソコン、モバイル端末を学習者用端末とする場合には、必要な対策を講じなければならない。

2　教育情報セキュリティ管理者は、盗難防止のため、教室等で利用するパソコンの管理等について物理的措置を講じるとともに、児童生徒が所有するパソコン、モバイル端末について自己管理の徹底を図らなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

3　教育情報セキュリティ管理者は、学習系システムへのログインパスワードの入力を必要とするように設定しなければならない。

4　統括教育情報セキュリティ責任者及び教育情報システム管理者は、児童生徒が学習者用端末を利用する際に不適切なサイトの閲覧を防止するための対策を講じなければならない。

5　教育情報セキュリティ管理者は、学習者用端末を校内でウェブ利用する児童生徒に対して、当該端末におけるマルウェア感染対策を講じるよう指導しなければならない。

6　教育情報セキュリティ管理者は、学校内における学習者用端末の運用ルールを策定しなければならない。

第６節　人的セキュリティ

（教職員の遵守事項）

第30条　教職員は、教育情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに教育情報セキュリティ管理者に相談し、指示を仰がなければならない。

2　教職員は、業務以外の目的で情報資産の外部への持ち出し、教育情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

3　教職員は、モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業については、次の内容を遵守しなければならない。

(1) 教職員は、学校のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、教育情報セキュリティ管理者の許可を得なければならない。

(2) 教職員は、外部で情報処理業務を行う場合には、教育情報セキュリティ管理者の許可を得なければならない。

4　教職員は、教員用端末以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用については、次の内容を遵守しなければならない。

(1) 教職員は、教員用端末以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、業務上必要な場合は、教育情報セキュリティ管理者の許可を得て利用することができる。

(2) 教職員は、教員用端末以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、外部で情報処理作業を行う際に安全管理措置を遵守しなければならない。

5　教育情報セキュリティ管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

6　教職員は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を教育情報セキュリティ管理者の許可なく変更してはならない。

7　教職員は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は教育情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒

体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。
８　教職員は、職員室等において、重要度Ⅱ以上の情報資産を取り扱う際には、児童生徒を含む外部からの入室者に情報が流出することがないように、必要な対策を行わなければならない。
９　教職員は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。
10　教職員は、児童生徒に対し、学習者用端末等を活用するにあたり、適切な指導をしなければならない。

（非常勤及び臨時の教職員への対応）
第31条　教育情報セキュリティ管理者は、非常勤及び臨時の教職員に対し、採用時にこの対策基準等のうち、非常勤及び臨時の教職員が守るべき内容を理解させ、また実施及び遵守させなければならない。
２　教育情報セキュリティ管理者は、非常勤及び臨時の教職員にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

（教育情報セキュリティポリシー等の掲示）
第32条　教育情報セキュリティ管理者は、教職員が常に教育情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

（外部委託事業者に対する説明）
第33条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、教育情報セキュリティポリシー及び実施手順のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

（情報セキュリティに関する研修・訓練）
第34条　CISOは、定期的に情報セキュリティに関する研修及び訓練を実施しなければならない。

（研修計画の策定及び実施）
第35条　CISOは、教育情報セキュリティ責任者と連携し、教職員に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、対策委員会の承認を得なければならない。
２　教育情報セキュリティ責任者は、新規採用の教職員を対象とする情報セキュリティに関する研修を実施しなければならない。
３　研修は、教育情報セキュリティ管理者、学校教育情報セキュリティ・システム担当者及びその他教職員に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。
４　CISOは、毎年度１回、対策委員会に対して、教職員の情報セキュリティ研修の実施状況について報告しなければならない。

（緊急時対応訓練）
第36条　CISOは、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

（情報セキュリティインシデントの報告）
第37条　教職員は、情報セキュリティインシデントを認知した場合、速やかに教育情報セキュリティ管理者に報告しなければならない。
２　報告を受けた教育情報セキュリティ管理者は、速やかに統括教育情報セキュリティ責任者及び教育情報システム管理者に報告しなければならない。
３　教育情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、必要に応じてCISO及び教育情報セキュリティ責任者に報告しなければならない。

（住民等外部からの情報セキュリティインシデントの報告）
第38条　教職員は、管理対象のネットワーク及び教育情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、教育情報セキュリティ管理者に報告しなければならない。
２　報告を受けた教育情報セキュリティ管理者は、速やかに統括教育情報セキュリティ責任者及び教育情報システム管理者に報告しなければならない。
３　教育情報セキュリティ管理者は、当該情報セキュリティインシデントについて、必要に応じてCISO及び教育情報セキュリティ責任者に報告しなければならない。

（情報セキュリティインシデント原因の究明・記録、再発防止等）
第39条　統括教育情報セキュリティ責任者は、情報セキュリティインシデントについて、教育情報セキュリティ管理者、教育情報システム管理者と連携し、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、CISOに報告しなければならない。
２　CISOは、統括教育情報セキュリティ責任者から、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

（IDの取扱い）
第40条　教職員は、自己の管理するIDに関し、次の事項を遵守しなければならない。
(1) 自己が利用しているIDは、他人に利用させてはならない。
(2) 共用IDを利用する場合は、共用IDの利用者以外が利用してはならない。
(3) その他のソフトウェア等の管理者用IDについては、教育情報セキュリティ管理者が指名するもの以外が利用してはならない。

（パスワードの取扱い）
第41条　教職員は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。
(1) パスワードは、他者に知られないように管理しなければならない。
(2) パスワードを秘密にし、パスワードの照会等には一切応じてはならない。
(3) パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。
(4) パスワードが流出したおそれがある場合には、教育情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。
(5) パスワードは定期的に又はアクセス回数に基づいて変更し、古いパスワードを再利用してはならない。
(6) 仮のパスワードは、最初のログイン時点で変更しなければならない。
(7) パソコンやモバイル端末等にパスワードを記憶させてはならない。
(8) 教職員間でパスワードを共有してはならない。ただし、共用IDに対するパスワードは除く。

第７節　技術的セキュリティ

（文書サーバ及び端末の設定等）

第42条　統括教育情報セキュリティ責任者は、教職員が使用できる文書サーバの容量を設定し、教職員に周知しなければならない。

２　統括教育情報セキュリティ責任者は、文書サーバを学校等の単位で構成し、教職員が他の学校等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

３　統括教育情報セキュリティ責任者は、児童生徒及び教職員の個人情報、人事記録等、特定の教職員しか取り扱えないデータについて、教育情報セキュリティ管理者の協力を得て、別途ディレクトリを作成する等の措置を講じ、同一学校等であっても、担当教職員以外の教職員が閲覧及び使用できないように設定しなければならない。

４　統括教育情報セキュリティ責任者は、インターネット接続を前提とする校務外部接続系サーバ及び学習系サーバに保管する情報（学習系サーバにおいては、機微な個人情報を保管する場合に限る。）については、標的型攻撃等によるファイルの外部流出の可能性を考慮し、ファイル暗号化等による安全管理措置を講じなければならない。

（バックアップの実施）

第43条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、次の事項に基づきバックアップを実施するものとする。

(1) 校務系情報及び校務外部接続系情報については、必要に応じて定期的にバックアップを実施しなければならない。

(2) 学習系情報については、必要に応じて定期的にバックアップを実施しなければならない。

（他団体との情報システムに関する情報等の交換）

第44条　教育情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、CISOの許可を得なければならない。

（システム管理記録及び作業の確認）

第45条　教育情報システム管理者は、所管する教育情報システムの運用において実施した作業について、作業記録を作成しなければならない。

２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

３　統括教育情報セキュリティ責任者、教育情報システム管理者又は教育情報システム管理者及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、２名以上で作業し、互いにその作業を確認しなければならない。

（情報システム仕様書等の管理）

第46条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失したりする等がないよう、適切に管理しなければならない。

（ログの取得等）

第47条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定期間保存しなければならない。

２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、ログとして取得す

る項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。
3　統括教育情報セキュリティ責任者及び教育情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

（障害記録）
第48条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

（ネットワークの接続制御、経路制御等）
第49条　統括教育情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。
2　統括教育情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

（外部ネットワークとの接続制限等）
第50条　教育情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、CISOの許可を得なければならない。
2　教育情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内及び学校の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。
3　教育情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保するように努めなければならない。
4　統括教育情報セキュリティ責任者及び教育情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、教育情報ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。
5　教育情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、CISOの判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（ネットワークの分離）
第51条　教育情報システム管理者は、校務系システム及び学習系システム間の通信経路の物理的又は論理的な分離をするとともに、校務系システム及び校務外部接続系システム間の通信経路を物理的又は論理的に分離し、それぞれで適切な安全管理措置を講じなければならない。
2　教育情報システム管理者は、校務系システム、校務外部接続系システム及び学習系システム間で通信する場合には、ウイルス感染のない無害化通信など、適切な措置を図らなければならない。

（複合機のセキュリティ管理）
第52条　統括教育情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定しなければならない。

２　統括教育情報セキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。
３　統括教育情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

（特定用途機器のセキュリティ管理）
第53条　統括教育情報セキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

（無線LAN及びネットワークの盗聴対策）
第54条　統括教育情報セキュリティ責任者は、無線LANの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。
２　統括教育情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

（電子メールのセキュリティ管理）
第55条　教育情報システム管理者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。
２　教育情報システム管理者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。
３　教育情報システム管理者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。
４　教育情報システム管理者は、教職員が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を教職員に周知しなければならない。
５　教育情報システム管理者は、システム開発や運用、保守等のため施設内に常駐している外部委託事業者の作業員による電子メールアドレス利用について、外部委託事業者との間で利用方法を取り決めなければならない。

（電子メールの利用制限）
第56条　教職員は、自動転送機能を用いて、電子メールを転送してはならない。
２　教職員は、業務上必要のない送信先に電子メールを送信してはならない。
３　教職員は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。
４　教職員は、重要な電子メールを誤送信した場合、教育情報セキュリティ管理者に報告しなければならない。
５　教職員は、ウェブで利用できるフリーメールサービス等を統括教育情報セキュリティ責任者の許可無しに使用してはならない。

（電子署名・暗号化）
第57条　教職員は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。
２　CISOは、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

（無許可ソフトウェアの導入等の禁止）
第58条　教職員は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。
２　教職員は、業務上の必要がある場合は、教育情報セキュリティ管理者の許可を得て、ソフトウェアを導入することができる。
３　教職員は、不正にコピーしたソフトウェアを利用してはならない。

（機器構成の変更の制限）
第59条　教職員は、パソコンやモバイル端末に対し、機器の改造及び増設・交換を行ってはならない。
２　教職員は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、統括教育情報セキュリティ責任者及び教育情報システム管理者の許可を得なければならない。

（無許可でのネットワーク接続の禁止）
第60条　教職員は、統括教育情報セキュリティ責任者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

（業務以外の目的でのウェブ閲覧の禁止）
第61条　教職員は、業務以外の目的でウェブを閲覧してはならない。
２　統括教育情報セキュリティ責任者は、教職員のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、教育情報セキュリティ管理者に通知し適切な措置を求めなければならない。

（アクセス制御等）
第62条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない教職員がアクセスできないように、システム上制限しなければならない。
２　利用者IDの取扱いについては、次の事項を遵守しなければならない。
(1) 統括教育情報セキュリティ責任者及び教育情報システム管理者は、利用者の登録、変更、抹消等の情報管理、教職員の異動、出向、退職に伴う利用者IDの取扱い等の方法を定めなければならない。
(2) 教職員は、業務上必要がなくなった場合は、利用者登録を抹消するよう、統括教育情報セキュリティ責任者及び教育情報システム管理者に通知しなければならない。
(3) 統括教育情報セキュリティ責任者及び教育情報システム管理者は、利用されていないIDが放置されないよう、人事管理部門と連携し、点検しなければならない。
３　特権を付与されたIDの管理等については、次の事項を遵守しなければならない。
(1) 統括教育情報セキュリティ責任者及び教育情報システム管理者は、管理者権限等の特権を付与されたIDを利用する者を必要最小限にし、当該IDのパスワードの漏えい等が発生しないよう、当該ID及びパスワードを厳重に管理しなければならない。
(2) 統括教育情報セキュリティ責任者及び教育情報システム管理者の特権を代行する者は、統括教育情報セキュリティ責任者及び教育情報システム管理者が指名し、CISOが認めた者でなければならない。
(3) CISOは、代行者を認めた場合、速やかに統括教育情報セキュリティ責任者、教育情報セキュリティ管理者及び教育情報システム管理者に通知しなければならない。
(4) 統括教育情報セキュリティ責任者及び教育情報システム管理者は、特権を付与されたID及びパスワードの変更について、外部委託事業者に行わせてはならない。
(5) 統括教育情報セキュリティ責任者及び教育情報システム管理者は、特権を付与されたIDを初期設定以外のものに変更しなければならない。

（教職員による外部からのアクセス等の制限）

第63条　教職員が外部から内部のネットワーク又は情報システムにアクセスする場合は、統括教育情報セキュリティ責任者及び教育情報システム管理者の許可を得なければならない。

２　統括教育情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

３　統括教育情報セキュリティ責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

４　統括教育情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

５　CISOは、公衆通信回線（公衆無線LAN等）を教育情報ネットワークに接続することは原則として禁止しなければならない。

（ログイン時の表示等）

第64条　教育情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ教職員がログインしたことを確認することができるようシステムを設定しなければならない。

（パスワードに関する情報の管理）

第65条　統括教育情報セキュリティ責任者又は教育情報システム管理者は、教職員のパスワードに関する情報を厳重に管理しなければならない。パスワードファイルを不正利用から保護するため、オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

２　統括教育情報セキュリティ責任者又は教育情報システム管理者は、教職員に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

（児童生徒のID及びパスワード等の管理）

第66条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、兵庫県教育委員会（以下「教育委員会」という。）又は学校が児童生徒に個別のIDを付与する場合、利用するクラウドサービス等のID及びパスワードに対して、次の事項を含めた適切な安全管理措置を講じなければならない。

(1) IDについては唯一無二、永続的に識別可能な構成とする。パスワードについては児童生徒の発達段階に応じて複雑性を上げたものとするなど、適切な措置を講じなければならない。

(2) 卒業、退学、転出等にクラウドサービス等の利用期間が終了する場合は、あらかじめ児童生徒本人によるデータ移行を利用期間内に実施し、アカウントの利用停止後、ID及び関連するデータの削除を行わなければならない。

（情報システムの調達）

第67条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（情報システムの開発）

第68条　教育情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。

２　システム開発の責任者及び作業者のIDの管理については、次の(1)及び(2)を遵守しなければならない。

(1) 教育情報システム管理者は、システム開発の責任者及び作業者が使用するIDを管理し、開発完了後、開発用IDを削除しなければならない。

(2) 教育情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

３　システム開発に用いるハードウェア及びソフトウェアの管理については、(1)及び(2)を遵守しなければならない。

(1) 教育情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

(2) 教育情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

（情報システムの導入）

第69条　開発環境と運用環境の分離及び移行手順の明確化については、次の事項を遵守しなければならない。

(1) 教育情報システム管理者は、システム開発・保守及びテスト環境とシステム運用環境を分離しなければならない。

(2) 教育情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

(3) 教育情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

(4) 教育情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

２　テストについては、次の事項を遵守しなければならない。

(1) 教育情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分なテストを行わなければならない。

(2) 教育情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

(3) 教育情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

(4) 教育情報システム管理者は、開発したシステムについて受け入れテストを行う場合、 開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

(5) 教育情報システム管理者は、運用環境への移行に先立ち、システムの脆弱性テストを行い、その結果を確認しなければならない。

（システム開発・保守に関連する資料等の整備・保管）

第70条　教育情報システム管理者は、システム開発・保守に関連する資料及びシステム関連文書を適切に整備・保管しなければならない。

２　教育情報システム管理者は、テスト結果を一定期間保管しなければならない。

３　教育情報システム管理者は、情報システムに係るソースコードを適切な方法で保管しなければならない。

（情報システムにおける入出力データの正確性の確保）

第71条　教育情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

２　教育情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

３　教育情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

（情報システムの変更管理）

第72条　教育情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

（開発・保守用のソフトウェアの更新等）

第73条　教育情報システム管理者は、開発・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

（システム更新又は統合時の検証等）

第74条　教育情報システム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

（不正プログラム対策に関する統括教育情報セキュリティ責任者の措置事項）

第75条　統括教育情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置しなければならない。

(1) 外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

(2) 外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

(3) コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ教職員に対して注意喚起しなければならない。

(4) 所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

(5) 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

(6) 不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

(7) 業務で利用するソフトウェアは、教育上特別な事情があり、教育情報セキュリティ管理者が許可した場合を除き、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。

（不正プログラム対策に関する教育情報システム管理者の措置事項）

第76条　教育情報システム管理者は、不正プログラム対策として、次の事項を措置しなければならない。

(1) 教育情報システム管理者は、その所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させなければならない。

(2) 不正プログラム対策ソフトウェア及びパターンファイルは、常に最新の状態に保たなければならない。
(3) インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、学校が管理している電磁的記録媒体以外を教職員に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

(不正プログラム対策に関する教職員の遵守事項)
第77条　教職員は、不正プログラム対策に関し、次の事項を遵守しなければならない。
(1) パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。
(2) 外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。
(3) 差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。
(4) 端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。
(5) 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。
(6) 統括教育情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。
(7) コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、以下の対応を行わなければならない。
ア　パソコン等の端末の場合
LANケーブルの即時取り外しを行わなければならない。
イ　モバイル端末の場合
直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。

(専門家の支援体制)
第78条　統括教育情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

(不正アクセス対策に関する統括教育情報セキュリティ責任者の措置事項)
第79条　統括教育情報セキュリティ責任者は、不正アクセス対策として、次の事項を措置しなければならない。
(1) 使用されていないポートを閉鎖しなければならない。
(2) 不要なサービスについて、機能を削除又は停止しなければならない。
(3) 不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括教育情報セキュリティ責任者及び教育情報システム管理者へ通報するよう、設定しなければならない。
(4) 統括教育情報セキュリティ責任者は、監視、通知、外部連絡窓口及び適切な対応等を実施できる体制並びに連絡網を構築しなければならない。

(攻撃の予告)
第80条　CISO及び統括教育情報セキュリティ責任者は、サーバ等に攻撃を受けることが明確になった場合、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

（不正アクセスに関する記録の保存）
第81条　CISO及び統括教育情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス行為の禁止等に関する法律（平成11年法律第128号）違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

（内部からの攻撃）
第82条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員及び外部委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（教職員による不正アクセス）
第83条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、教職員による不正アクセスを発見した場合は、当該教職員が所属する学校等の教育情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

（サービス不能攻撃）
第84条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

（標的型攻撃）
第85条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や事後対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

（セキュリティホールに関する情報の収集及び共有並びにソフトウェアの更新等）
第86条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

（不正プログラム等のセキュリティ情報の収集及び周知）
第87条　統括教育情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、教職員に周知しなければならない。

（情報セキュリティに関する情報の収集及び共有）
第88条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

第８節　運用

（情報システムの監視）
第89条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、セキュリティ

に関する事案を検知するため、情報システムを常時監視しなければならない。
２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

（教育情報セキュリティポリシーの遵守状況の確認及び対処）
第90条　統括教育情報セキュリティ責任者及び教育情報セキュリティ管理者は、教育情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかにCISOに報告しなければならない。
２　CISOは、発生した問題について、適切かつ速やかに対処しなければならない。
３　統括教育情報セキュリティ責任者及び教育情報システム管理者は、ネットワーク及びサーバ等のシステム設定等における教育情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

（パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査）
第91条　CISO及びCISOが指名した者は、不正アクセス、不正プログラム等の調査のために、教職員が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

（教職員の報告義務）
第92条　教職員は、教育情報セキュリティポリシーに対する違反行為を発見した場合、速やかに教育情報セキュリティ管理者に報告を行わなければならない。
２　報告を受けた教育情報セキュリティ管理者は、速やかに統括教育情報セキュリティ責任者及び教育情報システム管理者に報告しなければならない。
３　教育情報セキュリティ管理者は、報告のあった違反行為について、必要に応じてCISO及び教育情報セキュリティ責任者に報告しなければならない。
４　違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があるとCISO及び統括教育情報セキュリティ責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

（緊急時対応計画の策定）
第93条　CISOは、情報セキュリティインシデント、教育情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

（業務継続計画との整合性確保）
第94条　自然災害、大規模又は広範囲に及ぶ疾病等に備えて、対策委員会は業務継続計画とこの対策基準との整合性を確保しなければならない。

（緊急時対応計画の見直し）
第95条　CISOは、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

（例外措置の許可）
第96条　教育情報セキュリティ管理者及び教育情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、学校事務及び教育活動の適正な遂行を継続す

るため、遵守事項とは異なる方法を採用し又は遵守事項を実施しないことについて合理的な理由がある場合には、CISOの許可を得て、例外措置を取ることができる。

（緊急時の例外措置）

第97条　教育情報セキュリティ管理者及び教育情報システム管理者は、学校事務及び教育活動の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかにCISOに報告しなければならない。

（例外措置の申請書の管理）

第98条　CISOは、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

（法令等遵守）

第99条　教職員は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令等を遵守し、これに従わなければならない。

(1) 地方公務員法(昭和25年法律第261号)
(2) 教育公務員特例法（昭和24年法律第１号）
(3) 著作権法（昭和45年法律第48号）
(4) 不正アクセス行為の禁止等に関する法律（平成11年法律第128号）
(5) 個人情報の保護に関する法律（平成15年法律第57号）
(6) 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）
(7) 個人情報の保護に関する条例（平成８年条例第24号）

（懲戒処分等）

第100条　教育情報セキュリティポリシーに違反した教職員及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分等の対象とする。

（違反時の対応）

第101条　教職員の教育情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

(1) 統括教育情報セキュリティ責任者が違反を確認した場合は、統括教育情報セキュリティ責任者は当該教職員が所属する学校の教育情報セキュリティ管理者に通知し、適切な措置を求めなければならない。
(2) 教育情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括教育情報セキュリティ責任者及び当該教職員が所属する学校の教育情報セキュリティ管理者に通知し、適切な措置を求めなければならない。
(3) 教育情報セキュリティ管理者の指導によっても改善されない場合、統括教育情報セキュリティ責任者は、当該教職員の教育情報ネットワーク及び教育情報システムを使用する権利を停止又は剥奪することができる。その後速やかに、統括教育情報セキュリティ責任者は、教職員の権利を停止又は剥奪した旨をCISO及び当該教職員が所属する学校の教育情報セキュリティ管理者に通知しなければならない。

第９節　外部委託

（外部委託事業者の選定基準）

第102条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、外部委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

２　統括教育情報セキュリティ責任者及び教育情報システム管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

（契約項目）

第103条　情報システムの運用、保守等を外部委託する場合には、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

(1) 教育情報セキュリティポリシー及び実施手順の遵守
(2) 外部委託事業者の責任者、委託内容、作業者、作業場所の特定
(3) 提供されるサービスレベルの保証
(4) 外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法
(5) 外部委託事業者の従業員に対する教育の実施
(6) 提供された情報の目的外利用及び受託者以外の者への提供の禁止
(7) 業務上知り得た情報の守秘義務
(8) 再委託に関する制限事項の遵守
(9) 委託業務終了時の情報資産の返還、廃棄等
(10) 委託業務の定期報告及び緊急時報告義務
(11) 県による監査、検査
(12) 教育委員会による情報セキュリティインシデント発生時の公表
(13) 教育情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

（約款による外部サービスの利用に係る規定の整備）

第104条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、次の事項を含む約款による外部サービスの利用に関する規定を整備しなければならない。

(1) サービスを利用してよい業務の範囲
(2) 利用手続及び運用手順

（約款による外部サービスの利用における対策の実施）

第105条　教職員は、利用するサービスの約款、その他提供条件から、利用にあたってのリスクが許容できることを確認した上で約款による外部サービスの利用を教育情報セキュリティ管理者に申請し、適切な措置を講じた上で利用しなければならない。

（クラウドサービスの利用）

第106条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、教育委員会又は学校が管理するアカウントでクラウドサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたクラウドサービス運用方針を定めなければならない。

(1)クラウドサービス利用者は、クラウドサービス事業者と契約時に守秘義務、目的外利用及び第三者への提供の禁止条項を締結しなければならない。
(2)クラウドサービス事業者によるクラウドサービス利用者のログの収集は、原則、クラウドサービスのシステムを起動させるための基本情報とし、学習ログ等の個人情報を目的外の利用及び第三者に提供をしてはならない。

２　重要性Ⅰの情報資産は、クラウドサービスで発信、保存してはならない。ただし、統括教育情報セキュリティ責任者及び教育情報システム管理者が認めるクラウドサービスにおいて、統括教育情報セキュリティ責任者及び教育情報システム管理者が認める重要性Ⅰの情報資産を保存する場合は、この限りではない。

３　重要性Ⅱの情報資産を、クラウドサービスで発信、保存する場合は、教育情報セキュリティ管理者の許可を得なければならない。

４　利用するクラウドサービスごとに責任者を定めなければならない。

５　クラウドサービス利用者が、卒業、退学、転出、異動、退職等により利用をしなくな

った場合には該当アカウント及びクラウド上に保存している情報資産を削除、返却しなければならない。また、削除したIDは繰り返し利用してはならない。

（ソーシャルメディアサービスの利用）

第107条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、教育委員会又は学校が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

(1) 教育委員会又は学校が管理するアカウントによる情報発信が、実際の教育委員会又は学校のものであることを明らかにするために、教育委員会又は学校の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を行うこと。

(2) パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ICカード等）等を適切に管理するなどの方法で、不正アクセス対策を行うこと。

２　重要性Ⅱ以上の情報資産は、ソーシャルメディアサービスで発信してはならない。

３　利用するソーシャルメディアサービスごとの責任者を定めなければならない。

第10節　評価・見直し

（監査）

第108条　CISOは、情報セキュリティ監査統括責任者を指名し、教育情報ネットワーク及び教育情報システム等の情報資産における情報セキュリティ対策状況について、毎年度監査を行わせなければならない。

（監査を行う者の要件）

第109条　情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

２　監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

（監査実施計画の立案及び実施への協力）

第110条　情報セキュリティ監査統括責任者は、監査を行うにあたって、監査実施計画を立案し、対策委員会の承認を得なければならない。

２　被監査部門は、監査の実施に協力しなければならない。

（報告）

第111条　情報セキュリティ監査統括責任者は、監査結果を取りまとめ、対策委員会に報告しなければならない。

（保管）

第112条　情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

（監査結果への対応）

第113条　CISOは、監査結果を踏まえ、指摘事項を所管する教育情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない教育情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

（自己点検）

第114条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、所管するネットワーク及び情報システムについて、必要に応じて自己点検を実施しなければならない。

２　統括教育情報セキュリティ責任者は、教育情報セキュリティ管理者と連携して、所管する学校等における教育情報セキュリティポリシーに沿った情報セキュリティ対策状況について、必要に応じて自己点検を行わなければならない。

（報告）

第115条　統括教育情報セキュリティ責任者及び教育情報システム管理者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、対策委員会に報告しなければならない。

（自己点検結果の活用）

第116条　教職員は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

２　対策委員会は、自己点検結果をこの対策基準及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（対策基準及び関係規程等の見直し）

第117条　対策委員会は、監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、この対策基準及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。

附　則

１　この対策基準は、令和２年９月１日から施行する。

２　兵庫県教育情報ネットワーク運営管理要綱（平成11年４月１日制定）は、廃止する。

３　この対策基準は、令和４年４月１日から施行する。

４　この対策基準は、令和５年４月１日から施行する。

５　この対策基準は、令和６年４月１日から施行する。